JOURNAL OF NUMBER THEORY 54, 232–247 (1995)

The Index of a Point Lattice in a Set

B. UHRIN*

Computer and Automation Institute, Hungarian Academy of Sciences, 1518 Budapest, P.f. 63, Hungary

Communicated by Alan C. Woods

Received November 21, 1990; revised March 9, 1993

Let $L \subset R^n$ be an r-dimensional point lattice, $1 \leqslant r \leqslant n$, and $B \subset R^n$ be a measurable set. In the paper the index $[B : L]$ of L in B is introduced as the measure (or cardinality if it is finite) of the set of different residue classes modulo (L) intersecting B. Different descriptions of $[B : L]$ are given, basic properties of $[B : L]$ are studied, lower and upper estimations of $[B : L]$ are proved in the paper. © 1995 Academic Press, Inc.

1. INTRODUCTION

Let $L \subset M \subset R^n$ be two r-dimensional point lattices, $1 \leqslant r \leqslant n$, with bases $a_1, ..., a_r \in L$ and $b_1, ..., b_r \in M$, respectively. Then

$$a_i = \sum_{j=1}^{r} v_{ij} b_j, \qquad i = 1, 2, ..., r, \tag{1.1}$$

where v_{ij} are integers.

By a well known theorem (see, e.g., [1], pp. 11–15) to every (b_j) there is (a_i) and to every (a_i) there is (b_j), respectively, such that for v_{ij} in (1.1) we have

$$v_{ij} = 0 \quad \text{for } j > i \qquad \text{and} \qquad v_{ii} > 0 \quad \text{for } j = 1, ..., r. \tag{1.2}$$

The absolute value of the determinant of the matrix (v_{ij}) is called *the index of L in M* (see [1], [2], [4], [7], [15]). Denote this number by $[M : L]$.

(1.2) shows that

$$[M : L] = \prod_{1}^{r} v_{jj} \geqslant 1 \tag{1.3}$$

and $[M : L] = 1$ if and only $M = L$ (see, e.g., [7], pp. 45–52).

* E-mail: uhrin@ilab.sztaki.hu.

0022-314X/95 $12.00

Denoting by N the number of sublattices L of M having the given index $[M : L]$, we have

$$r^2 \cdot \log([M : L]) \geqslant \log N \tag{1.4}$$

(see [7], p. 51).

The definition of $[M : L]$ shows immediately that if $r = n$, then

$$[M : L] = \frac{dL}{dM}, \tag{1.5}$$

where dL, dM are the determinants of the lattices.

((1.5) serve for the definition of $[M : L]$ in a much more general setting, [15], p. 36.)

More interesting for us is the following identity, which can be proved using (1.2).

Let $\mathscr{L}$ be the set of all mutually disjoint residue classes modulo (L) in R^n. Each $w \in \mathscr{L}$ is a set of the form $L + x$ for some $x \in R^n$, hence $\mathscr{L}$ can be looked at as the collection of all mutually disjoint sets $L + x$, when x runs through R^n. In this paper we shall adopt rather this "geometric" point of view of $\mathscr{L}$ than the "algebraic" one identifying $\mathscr{L}$ with the quotient space R^n/L. So the elements of $\mathscr{L}$ give a disjoint decomposition of R^n.

Now, the mentioned identity is

$$[M : L] = |\{w \in \mathscr{L} : w \cap M \neq \varnothing\}|, \tag{1.6}$$

where $|H|$ means the cardinality of the set H (see, [1], p. 14 or [7], p. 49).

It is clear that there are infinitely many subsets D of M such that

$$\{w \in \mathscr{L} : w \cap M \neq \varnothing\} = \{w \in \mathscr{L} : w \cap D \neq \varnothing\}. \tag{1.7}$$

For any $S \subseteq M$ denote

$$[S : L] := |\{w \in \mathscr{L} : w \cap S \neq \varnothing\}|. \tag{1.8}$$

The relations (1.6) and (1.7) imply that for $D \subseteq M$ such that (1.7) holds we have

$$[M : L] = [D : L]. \tag{1.9}$$

It is also clear that to any $S \subseteq M$ there is $D \subset M$ such that

$$[S : L] = [D : L] = |D| \tag{1.10}$$

and that $[D:L]=|D|$ implies

$$(D-D)\cap L=\{\theta\}, \tag{1.11}$$

where θ is the zero vector and $D-D$ is the algebraic difference of D with itself.

For any $D\subset M$ such that $[D:L]=|D|$ we can write (taking into account (1.11)) the following two formal equations:

$$[D:L]\cdot(|(D-D)\cap L|+1)=2\,|D| \tag{1.12}$$

and

$$[D:L]\cdot(|(D-D)\cap L|-1)=|((D-D)\cap L)+D|-|D|, \tag{1.13}$$

where $E+F:=\{x+y: x\in E, y\in F\}$ denotes the algebraic sum of the sets $E, F\subset R^n$, in particular $E-E:=E+(-E)$ is the difference set.

The equations (1.12) and (1.13) are trivial consequences of (1.11).

It turns out that changing equations signs in (1.12) and (1.13) to $\geqslant$ and $\leqslant$, respectively, the resulting inequalities hold for any $D\subseteq M$ (see Theorem 3.1 in Section 3), so we get via (1.9), (1.10) a lower and an upper estimation for $[M:L]$.

In considerations above D need not be in M, the definition (1.8) of $[S:L]$ is meaningful for any at most countable set $S\subset R^n$ and for "continuously" many $D\subset R^n$ we have $[D:L]=[M:L]$.

This suggests a generalization of $[M:L]$ to any set $B\subset R^n$.

This paper is devoted to a detailed study of such a generalization.

2. The Definition and Basic Properties of $[B:L]$

Let $b_1, ..., b_r\in R^n$ be linearly independent and $L:=\{\sum_1^r u_i b_i: u_i \text{ integers}\}$ be the r-dimensional point-lattice generated by (b_i) (any r-dimensional point-lattice is of such a form). Let $\mathrm{lin}(L)$ be the linear subspace spanned by (b_i) and let $T\subset R^n$ be the orthogonal complement linear subspace to $\mathrm{lin}(L)$, i.e., $\mathrm{lin}(L)\oplus T=R^n$, where $\oplus$ is the direct sum. Denote $P:=Q\oplus T$ where $Q:=\{\sum_1^r \lambda_i b_i: 0\leqslant\lambda_i<1, i=1, ..., r\}$. P is a basic cell of L in R^n.

Let $\varphi: R^n\to P$ be the *canonical projection* defined by P, i.e., any point $y\in R^n$ can be written uniquelly in the form

$$y=\varphi(y)+[y], \qquad \varphi(y)\in P, \quad [y]\in L. \tag{2.1}$$

Let $\mathscr{L}$ be the family defined in the introduction. Then

$$|P \cap w| = 1, \qquad w \in \mathscr{L}, \tag{2.2}$$

i.e., there is a one-to-one correspondence between $\mathscr{L}$ and P.

Let $B \subset R^n$ be a Lebesgue measurable (shortly measurable) set. Let us call the number

$$[B : L] := m(\{x \in P : (L + x) \cap B \neq \varnothing\}) \tag{2.3}$$

the *index of L in B*, where

$$m(S) := \begin{cases} \mu(S) & S \subset R^n \text{ measurable not countable set} \\ |S| & S \subset R^n \text{ at most countable set,} \end{cases} \tag{2.4}$$

and μ is the Lebesgue measure in R^n.

One can easily check that

$$\{x \in P : (L + x) \cap B \neq \varnothing\} = \bigcup_{u \in L} (B - u) \cap P, \tag{2.5}$$

hence the set on the right hand side of (2.3) is measurable (both $[B : L] = 0$ and $[B : L] = \infty$ are admissible).

For any set $S \subseteq R^n$ denote

$$\varphi(S) := \{\varphi(y) : y \in S\}, \qquad [S] := \{[y] : y \in S\}. \tag{2.6}$$

We have

$$\varphi(S) = \{x \in P : (L + x) \cap S \neq \varnothing\} = \bigcup_{u \in [S]} (S - u) \cap P, \tag{2.7}$$

$$S = \bigcup_{u \in [S]} (S \cap (P + u)) \tag{2.8}$$

and

$$S = \bigcup_{x \in \varphi(S)} ((L + x) \cap S), \tag{2.9}$$

where the sets occurring in the unions in (2.8) and (2.9), respectively, are all non-empty and mutually disjoint.

Introduce the notations

$$S(k) := \{y \in S : |(L + y) \cap S)| = k\}, \qquad k = 1, 2, ..., \tag{2.10}$$

$$\hat{S}(k) := \{x \in P : |(L + x) \cap S| = k\}, \qquad k = 0, 1, ... \tag{2.11}$$

LEMMA 2.1. *Let $B \in R^n$ be measurable. Then $\hat{B}(k)$, $B(k)$, $k = 1, 2, \ldots$, are measurable and*

$$m(B(k)) = k \cdot m(\hat{B}(k)), \qquad k = 1, 2, \ldots. \tag{2.12}$$

Proof. Let $k \geq 1$ and let $[B][k]$ denote the family $\{h \subseteq [B] : |h| = k\}$, where $h, h' \in [B][k]$ are different if they differ by at least one element.

Put

$$\tilde{B}(h) := \Big(\bigcap_{u \in h} (B-u) \cap P \Big) \setminus \bigcup_{v \in [B] \setminus h} ((B-v) \cap P), \qquad h \in [B][k], \tag{2.13}$$

and

$$H[k] := \{h \in [B][k] : \tilde{B}(h) \neq \varnothing\}. \tag{2.14}$$

Then

$$\hat{B}(k) = \bigcup_{h \in H[k]} \tilde{B}(h) \tag{2.15}$$

and

$$B(k) = \bigcup_{h \in H[k]} \bigcup_{u \in h} (\tilde{B}(h) + u), \tag{2.16}$$

where

$$\tilde{B}(h) \cap \tilde{B}(h') = \varnothing, \qquad h, h' \in H[k]. \tag{2.17}$$

The sets $\tilde{B}(h)$ are measurable, hence (2.15), (2.16) imply that $\hat{B}(k)$, $B(k)$ are measurable and by (2.17) we have

$$m(\hat{B}(k)) = \sum_{h \in H[k]} m(\tilde{B}(h)) \tag{2.18}$$

and

$$m(B(k)) = \sum_{h \in H[k]} k \cdot m(\tilde{B}(h)). \tag{2.19}$$

This proves the lemma. ∎

COROLLARY 2.2.

$$m(\varphi(B)) = \sum_{k \geq 1} \frac{m(B(k))}{k}. \tag{2.20}$$

Proof. (2.7) shows that the non-empty members of the family $\{\hat{B}(k), k \geq 1\}$, are a disjoint decomposition of $\varphi(B)$. ∎

COROLLARY 2.3. *The quantity $m(\cdot)$ occurring in the definition* (2.3) *of* $[B : L]$ *does not depend on P but only on B and L.*

Proof. The right hand side of (2.3) is by (2.7) equal to $m(\varphi(B))$ and by (2.20) this quantity does not depend on P, because the right hand side of (2.20) does not depend on P. ∎

So an equivalent definition of $[B : L]$ is

$$[B : L] := m(\varphi(B)) \tag{2.21}$$

and by the previous corollary this quantity depends only on B and L.

ASSERTION 2.4. *Let $q \geq 1$ be integer and denote $P' := P - \sum_{i=1}^{r} (1/2)\, b_i$. Then*

$$[B : L] = (2q)^{-r} \cdot m((B + L) \cap 2qP'). \tag{2.22}$$

Proof. Denoting $H := \{\sum_1^r u_i b_i : -q \leq u_i < q,\ u_i \text{ integers}\} \subset L$ one can write $2qP' = P + H$. It is also clear that

$$B + L = \varphi(B) + L, \tag{2.23}$$

hence

$$(B + L) \cap 2qP' = \bigcup_{x \in \varphi(B)} (x + L) \cap (P + H). \tag{2.24}$$

But $(x + L) \cap (P + H) = x + H$ for $x \in \varphi(B) \subseteq P$, so we have

$$(B + L) \cap 2qP' = \varphi(B) + H. \tag{2.25}$$

The sets $\varphi(B) + u$, $u \in H$, are mutually disjoint and the cardinality of H is $(2q)^r$, hence (2.21) yields (2.22). ∎

It is clear that $[B : L]$ is translation invariant and monotone w.r.t. the set inclusion, i.e.,

$$[B : L] = [(B + y) : L], \qquad y \in R^n, \tag{2.26}$$

$$[B_1 : L] \leq [B_2 : L], \qquad B_1 \subseteq B_2 \subseteq R^n, \tag{2.27}$$

where, of course, in (2.27) either $\mu(\cdot)$ or $|\cdot|$ is used for both $[B_1 : L]$ and $[B_2 : L]$. For different $L - s$ we have

ASSERTION 2.5. *Let $L_1 \subset L_2 \subset R^n$ be two point-lattices of dimensions $r_1 \leqslant r_2$. Then*

$$[B : L_2] \leqslant [B : L_1] \tag{2.28}$$

and if

$$(B - B) \cap L_2 = (B - B) \cap L_1, \tag{2.29}$$

then

$$[B : L_2] = [B : L_1]. \tag{2.30}$$

Proof. First observe that

$$(L_1 + y) \cap B \subseteq (L_2 + y) \cap B, \qquad y \in R^n. \tag{2.31}$$

Denote the sets (2.10) for B, L_1 and L_2 by $B_1(k)$ and $B_2(k)$, respectively. (2.31) implies that

$$B_2(k) = \bigcup_{j=1}^{k} B_1(j) \cap B_2(k), \tag{2.32}$$

hence using (2.20) and (2.21) we can write

$$[B : L_2] = \sum_{k \geqslant 1} \sum_{j=1}^{k} \frac{m(B_1(j) \cap B_2(k))}{k}. \tag{2.33}$$

Similarly,

$$B_1(j) = \bigcup_{k \geqslant j} B_1(j) \cap B_2(k), \tag{2.34}$$

hence

$$[B : L_1] = \sum_{j \geqslant 1} \sum_{k \geqslant j} \frac{m(B_1(j) \cap B_2(k))}{j}. \tag{2.35}$$

These imply (2.28).

As to (2.30), if for some $y \in B$ we had $y' \in ((L_2 + y) \cap B) \setminus ((L_1 + y) \cap B)$, then $y' - y \in (B - B) \cap L_2$, and by the condition (2.29) we have $y' - y \in L_1$, consequently $y' \in (L_1 + y) \cap B$, a contradiction. So (2.29) and (2.31) imply $(L_1 + y) \cap B = (L_2 + y) \cap B$ for all $y \in B$, that gives, taking into account (2.20) and (2.21), the equality (2.30). ∎

3. Some Inequalities for $[B : L]$

Let us recall two known results. Let $\Lambda \subset R^n$ be an n-dimensional point-lattice, P be its basic cell and $B \subset R^n$ be a bounded measurable set. In [8] the set $P_B := \{x \in P : (B-x) \cap \Lambda \neq \varnothing\}$ has been introduced and it has been proved that

$$|(B-B) \cap \Lambda| \geqslant 2\frac{\mu(B)}{\mu(P_B)} - 1. \tag{3.1}$$

A converse estimation has been proved in [10]. Namely, for any $W \subset \Lambda$ such that $|W| = |(B-B) \cap \Lambda|$, we have

$$|(B-B) \subset \Lambda| \leqslant \frac{\mu(W; B) - \mu(B)}{\mu(P_B)} + 1, \tag{3.2}$$

where

$$\mu(W, b) := \int_{P_B} |W + ((B-x) \cap \Lambda)|\, dx. \tag{3.3}$$

While (3.1) is a sharpening of the classical Minkowski–Blichfeldt–v.d. Corput Theorem (see [2], [4]), (3.2) sharpens a result of Hadwiger, [5].

The set P_B is nothing else than $\varphi(B)$, so $\mu(P_B)$ is by (2.21) equal to $[B : \Lambda]$. Hence (3.1) and (3.2) turn to the following inequalities

$$\frac{2\mu(B)}{|(B-B) \cap \Lambda| + 1} \leqslant [B : \Lambda] \leqslant \frac{\mu(W, B) - \mu(B)}{|(B-B) \cap \Lambda| - 1}. \tag{3.4}$$

In what follows for any $B \subset R^n$ denote

$$b(y) := (L + y) \cap B, \qquad y \in R^n,$$

and

$$u := \sup\{|b(y)| : y \in B\}, \qquad l := \inf\{|b(y)| : y \in B\}.$$

It is clear that $y \in b(y)$ for $y \in B$, hence $l \geqslant 1$.

For any $y \in R^n$ let $d(y)$ mean the affine dimension of the set $b(y)$, by definition $d(y) = -1$ if $b(y) = \varnothing$. Recall that the affine dimension of the non-empty set $H \subset R^n$ is the maximum number of linearly independent vectors contained in the set $H - h$, where $h \in H$.

We have

$$d(y) = 0 \Leftrightarrow |b(y)| = 1 \tag{3.5}$$

and one can check easily that

$$|(B - B) \cap L| = 1 \Rightarrow u = 1. \tag{3.6}$$

THEOREM 3.1. *Let $B \subset R^n$ be a measurable set, $L \subset R^n$ be a point lattice of dimension r, $1 \leqslant r \leqslant n$. We have $[B : L] = 0$ if and only if $m(B) = 0$ and*

$$u = l < \infty \Rightarrow [B : L] = \frac{m(B)}{l}. \tag{3.7}$$

If B is such that $0 < m(B) < \infty$ and $1 < u < \infty$ then, denoting $D(B) := (B - B) \cap L$, for any $z \in B$ such that $u = |b(z)|$ we have

$$\frac{2m(B)}{|D(B)| + 1} \leqslant^1 \frac{2m(B)(d(z) + 1)}{2\,|D(B)| + d(z)^2 + d(z)} \leqslant^2 \frac{2m(B)(d(z) + 1)}{2\,|b(z) - b(z)| + d(z)^2 + d(z)}$$

$$\leqslant^3 \frac{m(B)}{u} \leqslant^4 \frac{u \cdot m(B) - m(B(u))}{u^2 - u} \leqslant^5 [B : L] \leqslant^6 m(B). \tag{3.8}$$

If B is such that $l < \infty$ then we have

$$[B : L] \leqslant^7 \frac{l \cdot m(B) + m(B(l))}{l^2 + l} \leqslant^8 \frac{m(B)}{l} \leqslant^9 m(B). \tag{3.9}$$

For any B we have

$$[B : L] \leqslant^{10} \frac{m(U + B) - m(B)}{|U| - 1} \leqslant^{11} m(B), \tag{3.10}$$

where $U \subset L$ is any finite set containing at least two elements.

$\leqslant^1$ is equality if and only if

$$d(z) = 1. \tag{3.11}$$

$\leqslant^4$ is equality if and only if

$$[B : L] = \frac{m(B)}{u}, \tag{3.12}$$

in which case $\leqslant^5$ is also equality.

If $u > l$ then $\leqslant^5$ is equality if and only if

$$\{\text{either } u = l+1 \text{ or } u \geqslant l+2 \text{ and } m(B(k)) = 0,\ l \leqslant k \leqslant u-2\}. \tag{3.13}$$

$\leqslant^6$ is equality if and only if

$$\{\text{either } u = l = 1 \text{ or } l = 1,\ u > 1 \text{ and } m(B(k)) = 0,\ 1 < k \leqslant u\}. \tag{3.14}$$

$\leqslant^8$ is equality if and only if

$$[B : L] = \frac{m(B)}{l}, \tag{3.15}$$

in which case $\leqslant^7$ is also equality.

$\leqslant^9$ is equality if and only if $l = 1$.

If $u > l$ then $\leqslant^7$ is equality if and only if

$$\{\text{either } u = l+1 \text{ or } u \geqslant l+2 \text{ and } m(B(k)) = 0,\ l+2 \leqslant k \leqslant u\}. \tag{3.16}$$

$\leqslant^{10}$ is equality if and only if

$$\{U = \{v, v+a, v+2a, \ldots\} \text{ and } \exists E \subseteq \varphi(B) \text{ s.t. } m(E) = m(\varphi(B)),$$
$$\text{and } b(x) = \{v(x), v(x)+a, v(x)+2a, \ldots\}\ \forall x \in E\} \tag{3.17}$$

The proof depends on the following three lemmas.

LEMMA 3.2. *For any at most countable non empty sets $H, E \subset R^n$ we have*

$$|E| + |H| - 1 \leqslant |E + H| \leqslant |E| \cdot |H| \tag{3.18}$$

and the first inequality in (3.18) *is equality if and only if $E = \{e, e+a, e+2a, \ldots\}$ and $H = \{h, h+a, h+2a, \ldots\}$ (i.e., both E and H are "arithmetical progressions" of the same "mesh").*

Proof. Clear (see remarks in the following section). ∎

LEMMA 3.3 [3]. *Let $H \subset R^n$ be an at most countable non empty set and let d be the affine dimension of H. Then*

$$|H - H| \geqslant (d+1) \cdot |H| - \frac{d(d+1)}{2}. \tag{3.19}$$

Proof. See [3] (and also remarks in the following section). ∎

LEMMA 3.4. *Let B, L be as in Theorem* 3.1. *Then*

$$\frac{u\cdot m(B)-m(B(u))}{u^2-u}\leqslant^5 [B:L]\leqslant^7 \frac{l\cdot m(B)+m(B(l))}{l^2+l}, \tag{3.20}$$

where $\leqslant^5$ and $\leqslant^7$ hold under the assumptions of (3.8) *and* (3.9), *respectively.*

If $u=l$, then both $\leqslant^5$ and $\leqslant^7$ are equalities. If $u>l$, then the exact conditions of equalities of $\leqslant^5$ and $\leqslant^7$ are (3.13) *and* (3.16), *respectively.*

Proof. The definition (2.10) of $B(k)$ shows that $B(k)=\varnothing$ for $k>u$ and $1\leqslant k<l$. The non-empty members of the family $\{B(k),\ l\leqslant k\leqslant u\}$ constitute a disjoint decomposition of B, hence

$$m(B)=\sum_{k\geqslant l}^{u} m(B(k)) \tag{3.21}$$

and by (2.20) and (2.21) we have

$$[B:L]=\sum_{k\geqslant l}^{u}\frac{m(B(k))}{k}. \tag{3.22}$$

The relations (3.21) and (3.22) imply that if $u=l$ then both inequalities in (3.20) turn to equalities.

If $u=l+1$ then using again (3.21) and (3.22) we get that

$$m(B)=(u-1)[B:L]+\frac{m(B(u))}{u}. \tag{3.23}$$

If $u\geqslant l+2$, then one can write the simple formal identity

$$m(B)=(u-1)\left(\frac{m(B(u))}{u}+\frac{m(B(u-1))}{u-1}+\sum_{k\geqslant l}^{u-2}\frac{m(B(k))}{u-1}\right)+\frac{m(B(u))}{u}. \tag{3.24}$$

The right hand side of (3.24) is clearly not greater than $(u-1)[B:L]+u^{-1}\cdot m(B(u))$ and it is equal to the latter term if and only if $m(B(k))=0$ for all $l\leqslant k\leqslant u-2$. This proves the first inequality in (3.20) and its exact conditions of equality as given by (3.13).

The proof of the second part of (3.20) is similar, but now we have to use the following identities:

If $u=l+1$ then

$$m(B)=(l+1)[B:L]-\frac{m(B(l))}{l}. \tag{3.25}$$

If $u \geqslant l+2$ then

$$m(B) = (l+1)\left(\frac{m(B(l))}{l} + \frac{m(B(l+1))}{l+1} + \sum_{k \geqslant l+2}^{u} \frac{m(B(k))}{l+1}\right) - \frac{m(B(l))}{l}. \tag{3.26}$$

Now the right hand side of (3.26) is not less than $(l+1)[B:L] - l^{-1} \cdot m(B(l))$ and is equal to the latter term if and only if $m(B(k)) = 0$ for all $l+2 \leqslant k \leqslant u$. This proves the second inequality in (3.20) and its exact conditions of equality (3.16). ∎

Proof of Theorem 3.1. The implication (3.7) is a simple consequence of (3.21) and (3.22).

First we prove (3.10).

The Lemma 2.1 implies that the function $|b(x)|$ of x is measurable on $\varphi(B)$ and

$$m(B) = \int_{\varphi(B)} |b(x)|\, dm(x), \tag{3.27}$$

where $\int_{\varphi(B)} |\cdot|\, dm(x)$ means Lebesgue integral when B is not countable and $\sum_{x \in \varphi(B)} |\cdot|$ when B is at most countable.

Denote $C := U + B$ and $c(y) := (L+y) \cap C$, $y \in R^n$. Then $\varphi(C) = \varphi(B)$ and using again the Lemma 2.1 we see that $|c(x)|$ is measurable on $\varphi(B)$ and

$$m(C) = \int_{\varphi(B)} |c(x)|\, dm(x). \tag{3.28}$$

For any $x \in \varphi(B)$ we have

$$c(x) = U + b(x), \tag{3.29}$$

hence applying the Lemma 3.2 we get

$$|b(x)| + |U| - 1 \leqslant |c(x)| \leqslant |U| \cdot |b(x)|, \qquad x \in \varphi(B), \tag{3.30}$$

and the exact conditions of equality in the first inequality as given in (3.17).

Integrating both sides of (3.30) over $\varphi(B)$ and taking into account (3.27), (3.28) and (2.21) we get (3.10) and (3.17).

To prove (3.8) and (3.9) observe that $b(z) - b(z) \subseteq D(B)$ and $u \geqslant d(z) + 1$. Hence, using Lemma 3.3 with $H := b(z)$, we get the following sequence of inequalities

$$|D(B)| \geqslant^{a} |b(z) - b(z)| \geqslant^{b} (d(z)+1) \cdot u - \frac{d(z)(d(z)+1)}{2}$$

$$\geqslant^{c} (d(z)+1)\frac{(d(z)+2)}{2} \geqslant^{d} (d(z)+1). \tag{3.31}$$

The left and right sides of (3.31) give

$$|D(B)|\,(d(z)-1) \geqslant^{c} (d(z)+1)(d(z)-1). \tag{3.32}$$

Now, the inequality $\leqslant^{1}$ in (3.8) is equivalent to (3.32). (3.31) implies that $\geqslant^{c}$ is strict for $d(z)>1$, which gives the condition (3.11).

The inequality $\leqslant^{2}$ in (3.8) is equivalent to $\geqslant^{a}$ in (3.31), while $\leqslant^{3}$ in (3.8) is equivalent to $\geqslant^{b}$ in (3.31).

$\leqslant^{4}$ is equivalent to $m(B) \geqslant m(B(u))$, which is by (3.21) equality if and only if

$$m(B(k))=0, \qquad l \leqslant k < u. \tag{3.33}$$

Taking into account (3.22), the latter condition is clearly equivalent to (3.12).

Similarly, $\leqslant^{8}$ in (3.9) is equivalent to $m(B) \geqslant m(B(l))$, which is (again by (3.21)) equality if and only if

$$m(B(k))=0, \qquad l < k \leqslant u \tag{3.34}$$

and by (3.22) this condition is equivalent to (3.15).

The inequalities $\leqslant^{5}$, $\leqslant^{7}$, in (3.8), (3.9) together with the exact conditions (3.13), (3.16) of them are proved in Lemma 3.4.

The remaining statements of the theorem are simple consequences of (3.21) and (3.22). ∎

Remark 3.5. A plausible sufficient condition of equality of $\leqslant^{11}$ is when $u+B$, $u \in U$, are all disjoint. A necessary condition would depend on having exact conditions for the equality of the second inequality in (3.18).

Similarly, exact conditions of the equality in $\leqslant^{3}$ of (3.8) depend on having such conditions for (3.19). Little is known about this problem (see, [3], [6] for more details).

Finally, exact conditions of the equality of $\leqslant^{2}$ in (3.8) depend on those of $\geqslant^{a}$ in (3.31), that also seems to be an interesting problem.

4. Remarks

4.1. The proof of (3.10) via (3.30) depends on the inequality (3.18). So any improvement of (3.18) yields an improvement of (3.10). Recently Ruzsa, [6], extended the result (3.19) by proving

$$|E+H| \geqslant |E| + d\,|H| - \frac{d(d+1)}{2}, \tag{4.1}$$

where $E, H \in R^d$ are finite sets, $|H| \leqslant |E|$ and $E+H$ is not contained in any lower dimensional hyperplane ((3.19) is the case $H=-E$ of (4.1)).

Using (4.1) for the set (3.29) one can prove improvements of (3.10) in some special cases of B.

AN EXAMPLE. If B, L are such that for all $x \in \varphi(B)$ we have (i) $|b(x)| \geqslant |U| \geqslant 2$ and (ii) the affine dimension of $b(x)+U$ is equal to d, then

$$[B:L] \leqslant \frac{2 \cdot m(U+B) - 2 \cdot m(B)}{2d \cdot |U| - d(d+1)}. \tag{4.2}$$

The right hand side of (4.2) is less than that of (3.10) provided $d>1$ and

$$|U| > \frac{d(d+1)-2}{2(d-1)}. \tag{4.3}$$

4.2. The comparison of the right hand sides of (3.10) and (3.9) leads to problems which are in some sense "converse" to (4.1). Denote

$$\Phi_1(U, B) := \frac{|U|+l}{l+1} m(B) + \frac{|U|-1}{l(l+1)} m(B(l))$$

and

$$\Phi_2(U, B) := \frac{|U|+l-1}{l} m(B),$$

where U, l are as in (3.10), (3.9).

One can easily check that

$$\Phi_1(U, B) \leqslant^{\alpha} \Phi_2(U, B) \leqslant^{\beta} |U| \cdot m(B), \tag{4.4}$$

$\leqslant^{\alpha}$ is equality if and only if

$$m(B) = m(B(l)) \tag{4.5}$$

and $\leqslant^{\beta}$ is equality if and only if $l=1$.

On the other hand $\leqslant^{11}$ of (3.10) reads as

$$m(U+B) \leqslant |U| \cdot m(B). \tag{4.6}$$

Now the comparison of right hand sides of (3.10) and (3.9) boils down to the "fitting" of $m(U+B)$ into (4.4).

Say, of $\Phi_1(U, B) = \Phi_2(U, B)$, then (4.5) implies $[B : L] = l^{-1} \cdot m(B)$ and (3.9) is (trivially) not "worse" than (3.10) because (3.10) $\leqslant^{10}$ is now equivalent to

$$\Phi_1(U, B) \leqslant m(U + B). \tag{4.7}$$

If $\Phi_1(U, B) < \Phi_2(U, B)$, then to find the proper "position" of $m(U + B)$ within (4.4) seems to be not an easy taks.

4.3. As to improvements of (3.8), these depend on finding improvements of (3.19). In the above mentioned paper of Ruzsa the following conjecture is posed.

Conjecture 4.1 [6]. Let $H \subset R^d$, $d \geqslant 3$, be a finite set and assume that H is not contained in any lower dimensional hyperplane. Then there are constants C_d depending only on d so that

$$|H - H| \geqslant 4.5\,|H| - C_3, \qquad d = 3 \tag{4.8}$$

and

$$|H - H| \geqslant \left(2d - 2 + \frac{2}{d}\right)|H| - C_d, \qquad d \geqslant 4. \tag{4.9}$$

If (4.8), (4.9) were true, then one could use them (analogously as (3.19) is used for (3.8)) to prove a sequence of inequalities of type (3.8).

4.4. In the Assertion 2.5 the behaviour of $[B : L]$ is described when L is changing. Another question is: For a fixed L, how does $[tB : L]$ behave as a function of $t > 0$? (Here $tB := \{tx : x \in B\}$.)

Using (2.21), the following statement can be read out of a result in [12]:

Assertion 4.2. Let $K \subset R^n$ be a bounded convex body and $L \subset R^n$ be an r-dimensional point lattice, $1 \leqslant r \leqslant n$. Then

$$[\lambda K : L] \leqslant \lambda^{n-r}[K : L], \qquad 0 \leqslant \lambda \leqslant 1. \tag{4.10}$$

4.5. A few words on the applications of the results of this paper.

The sequence of inequalities (3.8) together with the exact conditions of equalities in them as given in Theorem 3.1 can be used for investigations of the following two questions: (a) How "far" is $|(B - B) \cap L|$ from 1? (b) What is the structure of B (w.r.t. L) if $|(B - B) \cap L|$ is "near" to 1? The exploration of these questions on the base of Theorem 3.1 partly depend on exploring proper "geometric" contents of the conditions (3.11)–(3.17) of equalities in inequalities (3.8), (3.9), (3.10).

Many results on the magnitude of $|(B-B)\cap L|$ of quite various types can be found in [8]–[14].

As to applications of (4.10), improvements of the Successive Minima Theorem can be proved using (4.10) (for more details see [12]).

ACKNOWLEDGMENT

I thank the anonymous referee for his remarks concerning the first version of this paper. I have utilized them in writing the present improved version.

REFERENCES

1. J. W. S. CASSELS, "An Introduction to the Geometry of Numbers," Springer, Berlin/Göttingen/Heidelberg, 1959.
2. P. ERDŐS, P. M. GRUBER, AND J. HAMMER, "Lattice Points," Longman, London, 1989.
3. G. FREIMAN, A. HEPPES, AND B. UHRIN, A lower estimation for the cardinality of finite difference sets in R^n, *in* "Number Theory Budapest, 1987" (K. Győry, and G. Halász, Eds.), North-Holland, Amsterdam/New York, *Coll. Math. Soc. J. Bolyai* **51** (1989), 125–139.
4. P. M. GRUBER AND C. G. LEKKERKERKER, "Geometry of Numbers," 2nd ed., North-Holland, Amsterdam/New York, 1987.
5. H. HADWIGER, Überdeckung des Raumes durch translationsgleiche Punktmengen und Nachbarnzahl, *Monatsh. Math.* **73** (1969), 213–217.
6. I. Z. RUZSA, Sums of sets in several dimensions, *Combinatorica*, to appear.
7. C. L. SIEGEL, "Lectures on Geometry of Numbers," Springer, Berlin/Heidelberg/New York, 1967.
8. B. UHRIN, Some useful estimations in geometry of numbers, *Period. Math. Hungar.* **11** (1980), 95–103.
9. B. UHRIN, On a generalization of Minkowski convex body theorem, *J. Number Th.* **13** (1981), 192–209.
10. B. UHRIN, A remark to the paper of H. Hadwiger "Überdeckung des Raumes durch translationgleiche Punktmengen und Nachbarnzahl," *Monatsh. Math.* **104** (1987), 149–152.
11. B. UHRIN, Some remarks about the lattice points in difference set, *in* "Proc. of the A. Haar Memorial Conference, Budapest, 1985" (J. Szabados and K. Tandori, Eds.), North-Holland, Amsterdam/New York, *Coll. Math. Soc. J. Bolyai* **49** (1987), 929–937.
12. B. UHRIN, The measure of covering the Euclidean space by group translates of a set, *in* "The Mathematical Heritage of C. F. Gauss" (G. M. Rassias, Ed.), pp. 785–805, World Scientific Singapore, 1991.
13. B. UHRIN, New lower bounds for the number of lattice points in a difference set, *Acta Sci. Math. (Szeged)*, submitted for publication.
14. B. UHRIN, An analysis of the segment $[1, T]$, where T is the meeting number of a set-lattice, *Period. Math. Hungar.* **26** (1993), 139–156.
15. A. WEIL, "Basic Number Theory," Springer, Berlin/Heidelberg/New York, 1967.